

ABSTRACT OF THE DISCLOSURE

A method for controlling and tracking access to disseminated information involves encrypting data using a key that is maintained in a key repository. A user requests a message ID and key from the key repository. The key repository issues a message ID and key to the user. The user generates an encrypted message using the key. The encrypted message is then distributed with the message ID to one or more recipients. To read the encrypted message, a particular recipient obtains the key for the message from the key repository by providing the message ID to the key repository. The particular recipient then decrypts the message using the key provided by the key repository. Messages are deleted, in the sense of becoming unusable, by deleting the corresponding key from the key repository. A log is provided to track key repository activity including the issuance of keys and key requests from message recipients. A policy manager is employed to control which recipients are granted keys to read messages and which messages are deleted.